REMARKS

The February 6, 2006 Office Action rejected all of the pending claims. This Response amends claims 1, 2, 13-15, and 17-20, cancels claims 10 and 16, and introduces new claims 21-27. New independent claim 21 represents an amended and rewritten version of claim 10 (now cancelled), and new independent claim 25 is a method claim that recites subject matter contained in Applicant's original specification. No new matter has been introduced in the amendments or in the new claims. Amendments to the other pending claims improve the readability of the claims and/or clarify the claimed subject matter. After entry of the foregoing amendments, claims 1, 2, 6-9, 13-15, and 17-27 (20 total claims; 3 independent claims; no additional claim fees due) remain pending in the application. Reconsideration of the application is respectfully requested in view of the above amendments and the following remarks.

Claims 1, 2, 6, 7, 13-15, 17, and 18 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Toth et al, USPN 5,708,655 (hereinafter "Toth") in view of Ekberg, WO 00/02406 (hereinafter "Ekberg"). Claims 8, 9, 19, and 20 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Toth in view of Ekberg and further in view of Vilander et al., USPN 6,553,219 (hereinafter "Vilander") and the reference cited as "UMTS Release 1999, 3GPP" (hereinafter the "UMTS reference"). Applicant respectfully traverses these rejections as applicable to the amended and new claims.

Applicant's independent claim 1 recites a first network having a first security controller that selects one of a plurality of first network elements, and a second network having a second security controller that selects one of a plurality of second network elements. The security controllers establish a security association for the selected network elements and transmit the security association to the selected network elements. The transmission of the security association occurs dynamically on an as-needed basis in response to registration of a mobile device in the second network.

Applicant's independent claim 21 recites a secure communication method for a mobile device in an environment that includes a home network for the mobile device and a visited network for the mobile device, where the home network has a home network security controller and a plurality of home network elements, and where the visited network has a visited network security controller and a plurality of visited network elements. The recited method includes

registering the mobile device in the visited network, selecting a designated visited network element from the plurality of visited network elements, selecting a designated home network element from the plurality of home network elements, distributing, by the home network security controller, a designated security association to the designated home network element, and distributing, by the visited network security controller, the designated security association to the designated visited network element. The distribution of the designated security association occurs dynamically and on an as-needed basis.

Applicant's independent claim 25 also recites a secure communication method for an environment similar to that recited in claim 21. The method recited in claim 25 includes: pre-negotiating security associations for the home and visited network elements; maintaining, at the home network security controller, a pool of home network elements having respective pre-negotiated security associations; maintaining, at the visited network security controller, a pool of visited network elements having respective pre-negotiated security associations; and distributing a designated security association on an as-needed basis to a designated home network element and a designated visited network element. The designated home network element is contained in the pool of home network elements, and the designated visited network element is contained in the pool of visited network elements.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation to modify a reference or to combine the teachings of multiple references. Second, there must be a reasonable expectation of success. Third, the prior art must teach or suggest all of the recited claim limitations. Of course, the teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in Applicant's disclosure. Applicant respectfully submits that the Examiner has not met all of the above criteria.

Briefly, Applicant disagrees with the characterization of Toth and Ekberg contained in the Office Action. For example, the Office Action alleges that Toth teaches a secure communication system having a first security controller that selects one of a plurality of first network elements for coupling to a second network, and a second security controller that selects one of a plurality of second network elements for dynamically coupling to the first network element. To support this conclusion, the Office Action states that the gateway packet switch nodes (GPSNs) in Toth are akin to Applicant's recited security controllers because the GPSNs

provide encryption capabilities. Applicant respectfully disagrees with this comparison for the reasons set forth below. Moreover, the Office Action contends that Ekberg discloses security negotiation by first and second network security controllers, the establishment of security associations, and the transmission of security associations to the home and visited network elements, as recited by Applicant. Applicant respectfully disagrees with this reading of Ekberg for the reasons set forth below.

Toth discloses a wireless IP-based communication system that dynamically assigns IP addresses to a roaming mobile unit as a temporary address to route data (see Abstract). FIG. 1 of Toth depicts the home network 12, which serves as the home network for a mobile unit 32, and a visited network 14 (this network is a visited network from the perspective of a mobile unit 52, i.e., network 14 is not the home network for the mobile unit 52). The focus of Toth is to provide a temporary IP address for the mobile unit 52 while the mobile unit 52 is in the visited network 14. This temporary IP address enables data to be routed from the fixed host device 54 (in the home network 12), through the visited network 14, and to the mobile unit 52 without having to route the data to the GPSN 26 of the home network 12. FIG. 4 of Toth depicts the supposedly inefficient routing of data that the Toth system solves. In FIG. 4, data from the fixed host 54 must first be routed to the GPSN 26 of the home network. Thereafter, the GPSN 26 routes the data to the visited network, which then routes the data to the roaming mobile unit 52. In contrast, FIG. 1 of Toth represents the solution proposed by Toth, namely, once the temporary IP address for the mobile unit 52 has been assigned, data between the fixed host 54 and the mobile unit 52 is only routed through the visited network 14. In other words, the data is not routed to the GPSN 26 of the home network 12.

The Office Action (on Page 2) contends that the GPSNs disclosed by Toth function as "security controllers" as recited by Applicant. To support this conclusion, the Office Action merely states that Toth's GPSN "consists of a cipher mode . . . therefore, the GPSN functions as a security controller since it provides encryption capabilities. The cipher mode is a type of "security mechanism" as stated in applicant's specification." Applicant respectfully disagrees with this characterization of Toth.

Although Applicant acknowledges that Toth's GPSNs support a cipher mode that may relate to security, the GPSNs do not otherwise function as recited in Applicant's claims. In this regard, the cipher mode mentioned in Toth is utilized during authentication of the mobile

telephone (identified as MT in Toth's FIG. 2). FIG. 2 of Toth clearly depicts that the cipher mode is used between the mobile telephone and the GPSN 46 during the authentication procedure. Referring also to Toth's FIG. 1, this authentication procedure is exclusively supported by the visited network 14, i.e., this authentication process does not involve the home network 12 at all. In fact, none of the operating components depicted in Toth's FIG. 2 (the vertical lines represent the operating components) are components in the home network 12. In other words, Toth's cipher mode is not utilized to support secure network-to-network communication. In contrast, Applicant's security controllers are configured to establish a designated security association and to transmit or distribute that security association dynamically and on an as-needed basis to support secure communication between the home network and the visited network. Toth simply does not teach or suggest this feature.

The Office Action (on Pages 2-3) also states that "Toth is directed towards tunneling a connection from one network to another" (citing Toth at Column 7, Line 61 to Column 8, Line 11). The Office Action also states here that tunneling "consists of coupling two network elements together." The Office Action uses these statements to support the proposition that Toth teaches security controllers that select network elements to be coupled to each other. Applicant respectfully disagrees with this conclusion. As discussed above, the Office Action contends that Toth's GPSNs function as Applicant's security controllers. For consistency with this comparison, therefore, Toth's GPSNs must also perform the selecting of the network elements and the transmission/distribution of the designated security association to the selected network elements, where the transmission/distribution of the security association is performed dynamically on an as-needed basis (as recited in Applicant's claims). Toth's GPSNs fall well short of this recited functionality and configuration. Simply put, Applicant's claims recite security controllers and corresponding network elements coupled to and controlled by the respective security controllers; for a given network (the home network or the visited network), the security controller is distinct and different from the network elements. In particular, Toth does not teach a GPSN that dynamically selects a different network element (i.e., not itself) on an as-needed basis, where that selected network element communicates with a counterpart network element in another network.

Regarding Ekberg, the Office Action contends that Ekberg discloses security negotiation by first and second security controllers (citing Ekberg at Page 7, Lines 11-23), and

that Ekberg discloses security controllers that establish security associations between network elements and then transmit the security associations to the network elements (citing Ekberg at Page 7, Lines 11-23, and at Page 8, Lines 13-24). Applicant respectfully disagrees with this characterization of Ekberg. As best understood, Ekberg does not teach the use of two security controllers, where one is resident in the home network and one is resident in the visited network. The cited excerpt of Ekberg mentions the use of a security server in the GSM network, but it does not disclose two different security controllers in the mobile networks as recited in Applicant's claims. Moreover, as best understood, Ekberg does not teach security controllers that establish and transmit security associations to the respective home/visited network elements. Rather, Ekberg relates to the authentication of the mobile terminal when registering in a subnetwork. Although FIG. 2 of Ekberg depicts the communication of a registration request (RR) message and a reply message between the home agent (in the home network) and the foreign agent (in the foreign network), there is no mention of security associations transmitted or distributed to the home/foreign network elements from respective security controllers within the home/foreign networks. Consequently, the cited excerpts of Ekberg do not support the conclusions reached by the Office Action. If the Office decides to maintain the claim rejections based upon this characterization of Ekberg, then Applicant respectfully requests the Office to support its reliance on Ekberg with an element-by-element comparison of the features and functions of Ekberg that allegedly correspond to the limitations recited in Applicant's claims.

Regarding Applicant's independent claims 1, 21, and 25, Toth as a primary reference fails to teach or suggest a number of recited limitations, and Ekberg, Vilander, and the UMTS reference do not compensate for the shortcomings of Toth. Indeed, even if a person skilled in the art were to combine or modify these three references, that person would not arrive at any of Applicant's recited independent claims. For the same reasons, that person would not arrive at any of Applicant's dependent claims.

Regarding claims 13, 14, and 25, the cited combination of references neither teaches nor suggests the pooling of home/visited network elements having respective pre-negotiated security associations. The Office Action (at Page 6, item 5) briefly concludes that Toth discloses network pooling, citing Toth at Column 9, Lines 34-44. Applicant disagrees with this conclusion and its application to any of Applicant's claims. To the extent Toth teaches

"network pooling" at all, such pooling relates to the pooling of "unused IP addresses" and such pooling does not refer to the pooling of network elements having certain pre-negotiated security associations. The rejection of claims 13 and 14 on this basis is improper and Applicant respectfully requests the Office to reevaluate its characterization of Toth in this context. Consequently, claims 13, 14, and 25-27 are allowable for these additional reasons.

Moreover, the cited combination of references neither teaches nor suggests the termination of the designated security association at the selected network elements in response to the termination of the current multimedia services maintained between the two networks (as recited in Applicant's claims 23 and 24. This feature relates to the dynamic and real-time nature of the recited security technique, which distributes a given security association on an as-needed basis in response to registration of the mobile device in different networks. Similarly, the cited combination of references neither teaches nor suggests the changing of the designated security association when the mobile device registers in another network (as recited in Applicant's claim 26). Likewise, the cited combination of references neither teaches nor suggests the maintaining of the secure communication path only for the duration that the mobile device is registered in the current visited network (as recited in Applicant's claim 27). Consequently, each of claims 23, 24, 26, and 27 are allowable for these additional reasons.

For at least the above reasons, all of the pending claims are patentable over Toth, Ekberg, Vilander, and any reasonable combination thereof. In particular, claims 1, 2, 6, 7, 13-15, 17, and 18 are not unpatentable over Toth in view of Ekberg, claims 8, 9, 19, and 20 are not unpatentable over Toth in view of Ekberg and further in view of Vilander and the UMTS reference, and new claims 21-27 are patentable over these references. Accordingly, all claims now presently in the application are believed allowable and such allowance is respectfully requested. Should the Examiner have any questions or wish to further discuss this application, Applicants request that the Examiner contact the undersigned attorney at (480) 385-5060.

If for some reason Applicants have not requested a sufficient extension and/or have not paid a sufficient fee for this response and/or for the extension necessary to prevent abandonment on this application, please consider this as a request for an extension for the required time period and/or authorization to charge Deposit Account No. 50-2091 for any fee which may be due.

Respectfully submitted,

If for some reason Applicants have not requested a sufficient extension and/or have not paid a sufficient fee for this response and/or for the extension necessary to prevent abandonment on this application, please consider this as a request for an extension for the required time period and/or authorization to charge Deposit Account No. 50-2091 for any fee which may be due.

Respectfully submitted,

INGRASSIA FISHER & LORENZ

Dated: June 6, 2006

By: _____

Mark M. Takahashi
Reg. No. 38,631
(480) 385-5060